



Network Security: The Future

Dr. Eric Cole
Chief Scientist
The Sytex Group, Inc.
ecole@atrc.sytexinc.com




Current Day: 2004 The _____ Worm

- ♦ Major worm impacted the operation of the Internet.
- ♦ Threat/Vulnerabilities:
 - Poor Perimeter Protection
 - Minimal Defense in Depth
 - Ineffective patching/fixing of known vulnerabilities
 - Running multiple services on the same system
- ♦ Countermeasures
 - Apply a principle of least privilege
 - Understand perimeter
 - Multiple Levels of protection
 - Timely prevention and detection



Rewind: 1988 The Morris Worm

- ♦ Major worm impacted the operation of the Internet.
- ♦ Threat/Vulnerabilities:
 - Poor Perimeter Protection
 - Minimal Defense in Depth
 - Ineffective patching/fixing of known vulnerabilities
 - Running multiple services on the same system
- ♦ Countermeasures
 - Apply a principle of least privilege
 - Understand perimeter
 - Multiple Levels of protection
 - Timely prevention and detection



Analysis: General

- ♦ Functionality wise we have made major strides in the last 15 years
- ♦ Security wise we have made minimal progress
- ♦ We are not learning from our mistakes and worse, we are making the same mistakes over and over again

Analysis: Security Solutions

- ♦ Security is not about products, solutions or dollars
- ♦ Security is about risk to critical assets
- ♦ Implementing firewalls, intrusion detection, intrusion prevention and other solutions with minimal knowledge of your organization will do minimal in terms of protecting your critical assets

Bad News

- ♦ Something has to give
- ♦ Two possibilities:
 - Things get worse
 - Things get better

Good News

- ♦ Organizations are now realizing the threat is real
- ♦ A monetary value can be assigned to an attack and cost benefit analysis can be performed
- ♦ Security spending is increasing
- ♦ So, is getting attacked, really a bad thing

Things Get Worse

- ♦ Massive attack vector
- ♦ Some possibilities:
 - Major back door in popular infrastructure OS
 - DNS
 - Routing
 - Coordinated Denial of Service attack against e-commerce infrastructure

Things Get Better

- ♦ Everyone likes to blame the vendors...
- ♦ Organizations have to better understand:
 - Threats and corresponding vulnerabilities
 - Security solutions require products and people
 - Security is not plug and play
 - Defense in depth is critical

What is on the Horizon? (Cont.)

- ♦ Insider attack becoming major attack vector
 - Most solutions focused on perimeter
- ♦ Corporate Espionage
- ♦ Patching
 - Fix the known before going after the unknown
- ♦ Understanding and managing risk

What is on the Horizon?

- ♦ Better coordination among security devices.
 - Enterprise Security Management starting to become a reality
- ♦ Merging of independent functionality across systems
 - Firewall + IDS = IPS
- ♦ More intelligent systems
 - Autonomic computing, self-healing, self-defending, self-configuring
- ♦ Convergence
 - PBX and Network Backbone merged
- ♦ Validation and control
 - Making sure things do not get worse

Potential Pitfalls

- ♦ Regulations
 - Could help or could focus attention on non-critical areas
 - Trying to fix the problem solely with laws
- ♦ Too much dependence on technology
- ♦ Waiting for proof there is a problem
 - Forces reactive measures as opposed to proactive measures
- ♦ Not thinking out of the box



Gregory Mita 2002

Security ????

- ◆ Where are we at in the bell curve?
- ◆ Will network security ever become a commodity, like physical security is in some domains?
- ◆ Is security just the next revenge of the nerds like Y2K?
- ◆ Will security just merge into a compliance and auditing role?



Gregory Mita 2002

Questions????

Dr. Eric Cole
Chief Scientist
The Sytex Group, Inc.
ecole@atrc.sytexinc.com